RESEARCH DATA ALLIANCE

Blockchain Applications in Health WG@P14

Regulatory and Legal Issues Related to Blockchain Applications in Health and "Decision Tree" Improvement

25 October 2019, 9:00-10:30

Co-Chair: Edwin Morley-Fletcher

research data sharing without barriers

rd-alliance.org

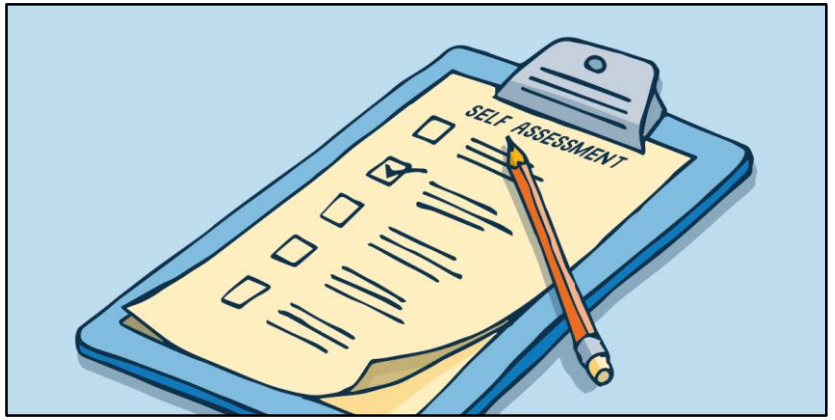
PANETTA & ASSOCIATI
STUDIO LEGALE

Security, Privacy & Legal aspects of Healthcare Big Data Analytics within the General Data Protection Regulation

Helsinki, October 25th, 2019

GOLDEN RULE : ACCOUNTABILITY

The main innovation introduced by the EU *General Data Protection Regulation* 2016/679 is the strengthening of the concept of accountability. **The data controller must be able to demonstrate compliance with the obligations imposed by the GDPR**, with particular reference to the principles of (a) **lawfulness**, **fairness** and **transparency**; (b) **purpose limitation**; (c) **data minimization**; (d) **accuracy**; (e) **storage limitation**; (f) **integrity and confidentiality**.



Before GDPR

MUST DO…

25th May 2018

PROVE THAT YOU DID…

DATA PROTECTION IMPACT ASSESSMENT

The controller must carry out a thorough and detailed assessment of the impacts (Data Protection Impact Assessment – 'DPIA') that the envisaged processing activities may produce, especially if based on new technologies, when they may results in significant risks to the security, rights and freedoms of the data subjects involved.

Basic elements of a DPIA:

- A systematic evaluation of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the rights and freedoms of the persons concerned (data subjects);
- The measures provided to address the risks, with a specific indication of the safeguards, security measures and mechanisms adopted to ensure the protection of personal data and to demonstrate compliance with GDPR.

DATA PROTECTION IMPACT ASSESSMENT

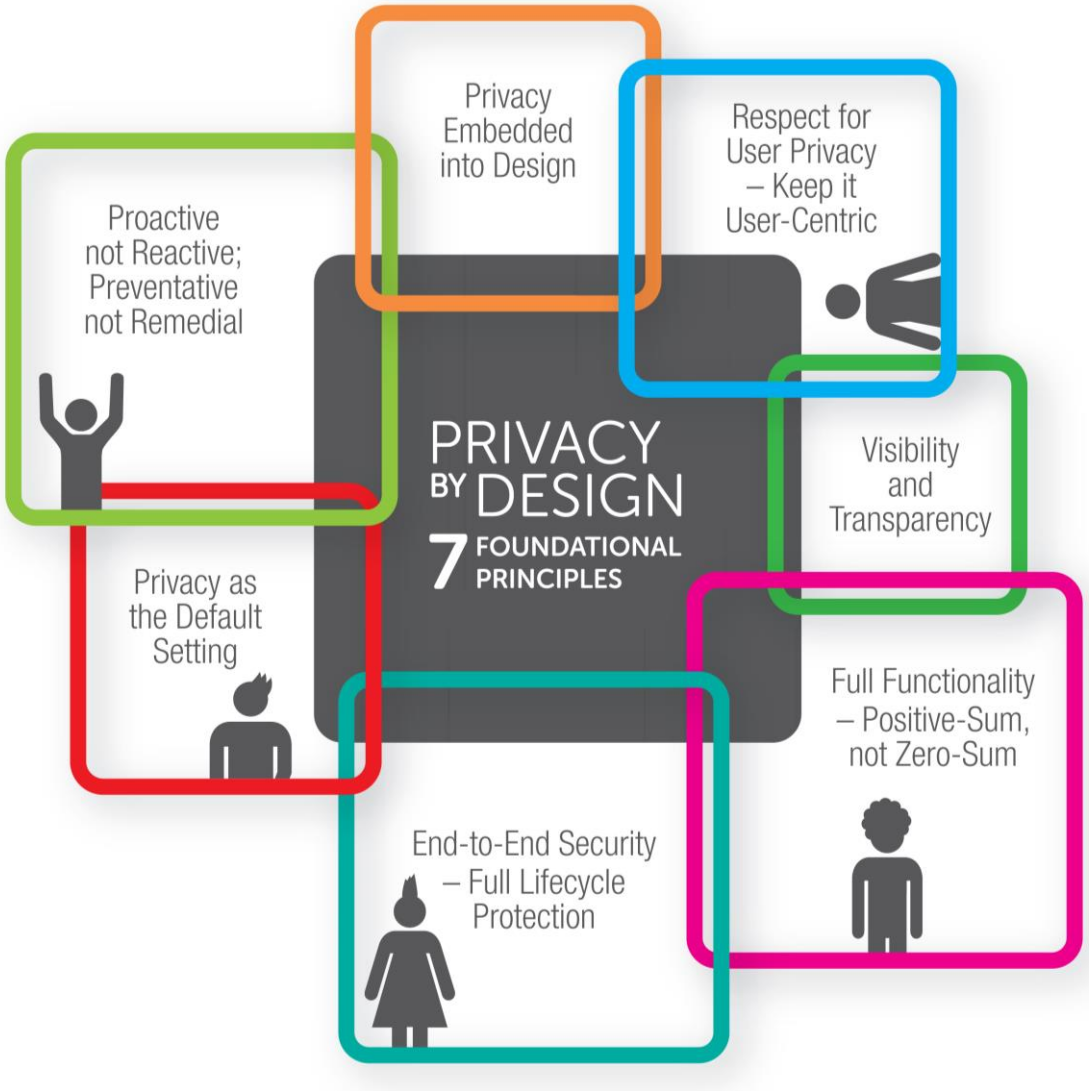
When a company innovates its processes, brings new services to the market or implements new methods of production or service, the protection of personal data must be taken into the utmost account and evaluated, not as a bureaucratic formality, but as a structural phase of the innovation process which contributes, together with more traditional ones, to the overall assessment of the innovation's sustainability.

Designing, making use or marketing new technologies (e.g. homomorphic encryption, secure multiparty computation, blockchain, smart contracts, etc.) obliges their developer, manufacturer or seller, as data controllers, to carry out a data protection impact assessment aimed to weigh up and identify any threats which may arise from the underlying data processing activities, in order to prevent or at least minimize such risks.

NEW TECHNOLOGIES: PRIVACY-BY DESIGN AND PRIVACY-BY-DEFAULT

PRIVACY-BY-DESIGN

Taking into account the state of the art, the cost of implementation and the nature, scope, context, purposes and risks of the processing, the controller must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures aimed at ensuring compliance with the data-protection principles.



PRIVACY-BY-DEFAULT

The controller must implement appropriate technical and organisational measures for ensuring that, by default, only those personal data which are necessary to achieve the intended purposes are processed, in relation to, among other elements, the volume of data collected, the period of their storage, the scope of the processing activities and the permissions to access the datasets

SECURITY MANAGEMENT: WHICH MEASURES SHOULD BE TAKEN?

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, **the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including *inter alia* as appropriate: a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures ensuring the security of the processing.

In assessing of adequacy of the security level, particular account shall be taken of the risks arising from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data.

THE CHAIN OF FUNCTIONS AND RESPONSIBILITIES

A fundamental objective must be setting up a correct chain of responsibilities for all service providers, distributors, agents, outsourcers, commercial partners and, more generally, external parties involved in different ways in the execution of business activities and, therefore, in data processing and security management.

Security chain

DATA CONTROLLER

The natural or legal person that, alone or together with others, collects the personal data and has the power to decide regarding modalities, purposes and security standards of processing

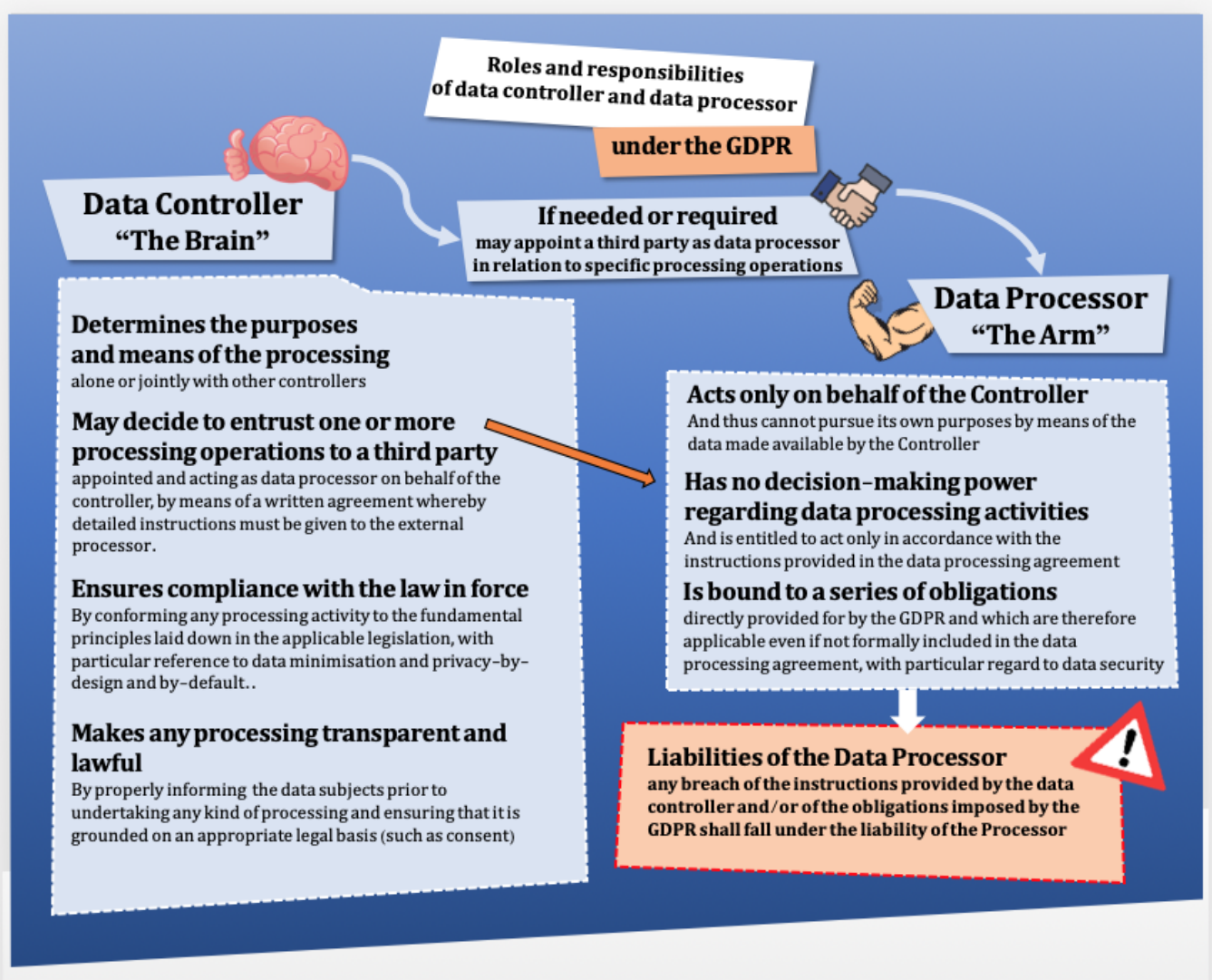
DATA PROCESSOR

The natural or legal person that processes data only by written "delegation" of the controller and therefore exclusively on behalf of and according to instructions of the controller

PERSON AUTHORIZED TO PROCESS THE DATA

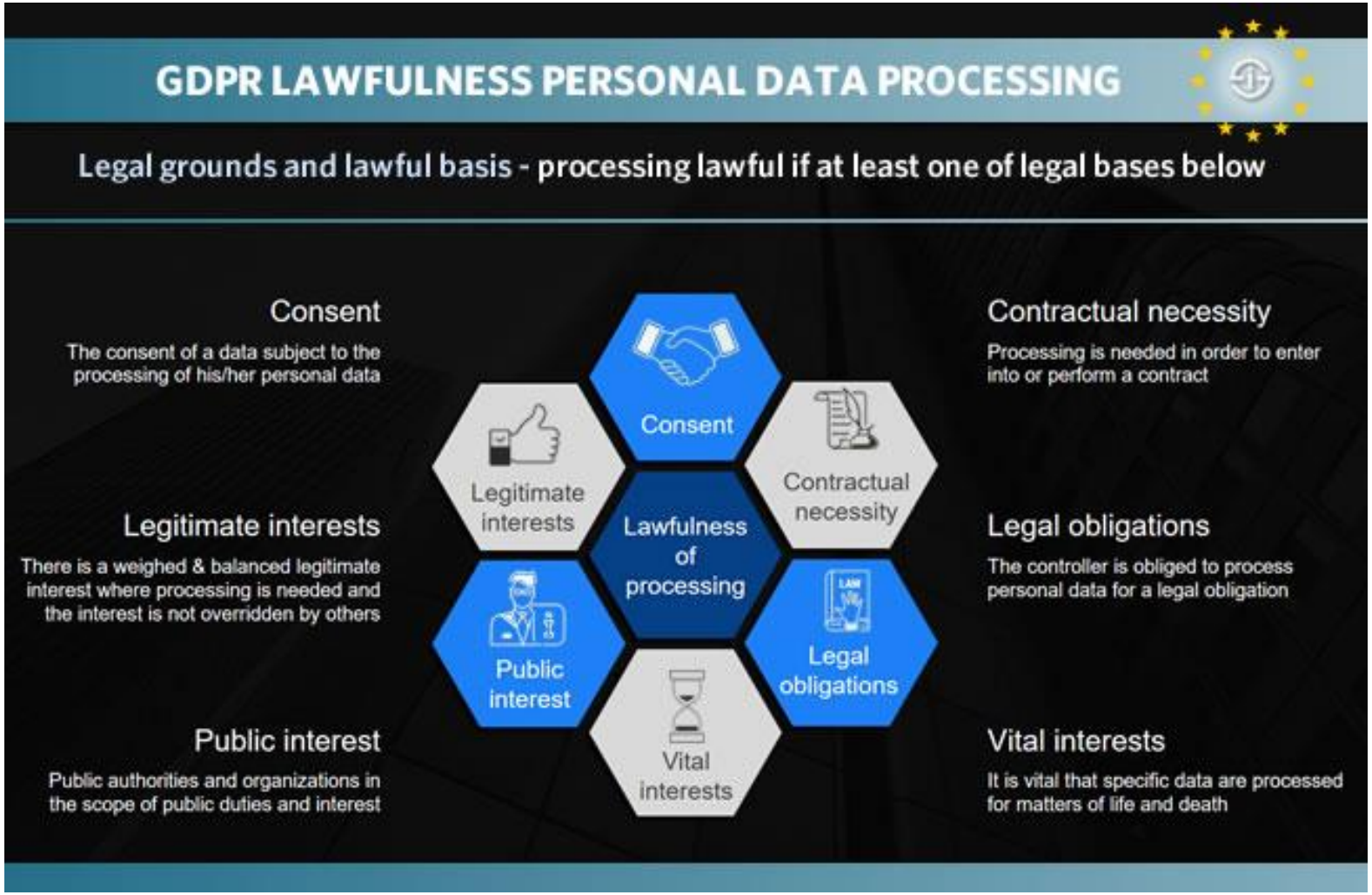
The natural person, operating under the authority of the controller or processor (e.g. employees, collaborators), who materially executes the data processing operations

DATA CONTROLLER AND DATA PROCESSOR

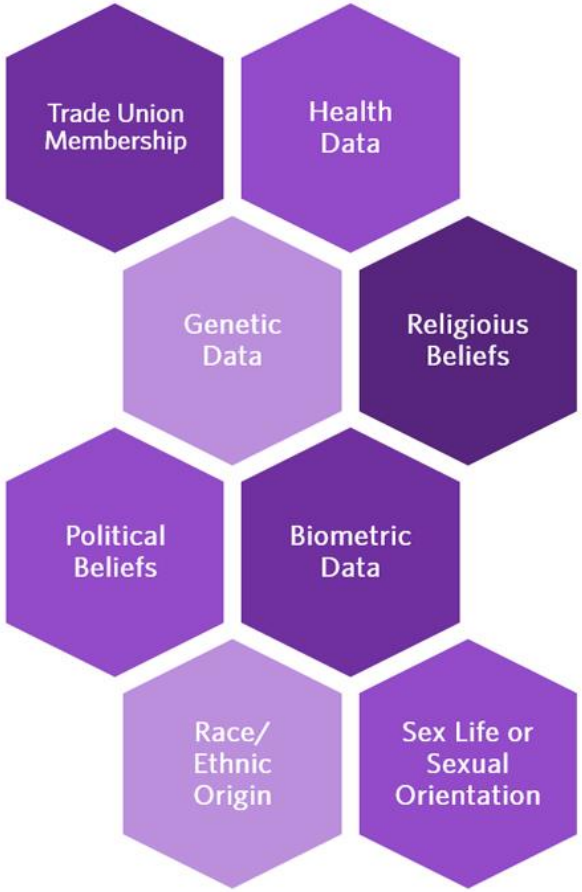


The execution of one or more operations which imply the processing of personal data can be entrusted by the controller to capable, reliable and trusted external service providers designated as data processors and bound to comply with the instructions given by the controller and with a wide series of obligations set forth in the GDPR.

LEGAL BASES WHICH ENSURE THE LAWFULNESS OF THE PROCESSING: ART. 6 OF THE GDPR



LEGAL BASES WHICH ENSURE THE LAWFULNESS OF THE PROCESSING: ART. 9 OF THE GDPR



It is prohibited to process special categories of data unless specific conditions are satisfied which ensure the lawfulness of the processing, e.g. with reference to the health sector, when the processing is necessary:

- ✓ for reason of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of data subject, in particular professional secrecy;
- ✓ for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89.1 based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

SCIENTIFIC AND MEDICAL RESEARCH UNDER THE GDPR

REUSE FOR RESEARCH PURPOSES

The GDPR establishes that **further processing for scientific research purposes must «*not be considered to be incompatible with the initial purposes*», so long as technical and organisational measures have been put in place** to ensure that: a) only those personal data will be processed which are strictly necessary to pursue the research purposes (data minimization) and, b) strict functional separation between participants in the research and outside stakeholders, meaning that data used for research purposes must not be made available for other kind of processing activities

Sensitive data

When the research involves any special category of data (e.g. health data), the application of flexible approach should be subject to a stricter interpretation, requiring a high degree of scrutiny

'Broad consent'

As it is often impossible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection, **data subjects should be allowed to give their consent to certain areas of scientific research** when in keeping with recognised ethical standards.

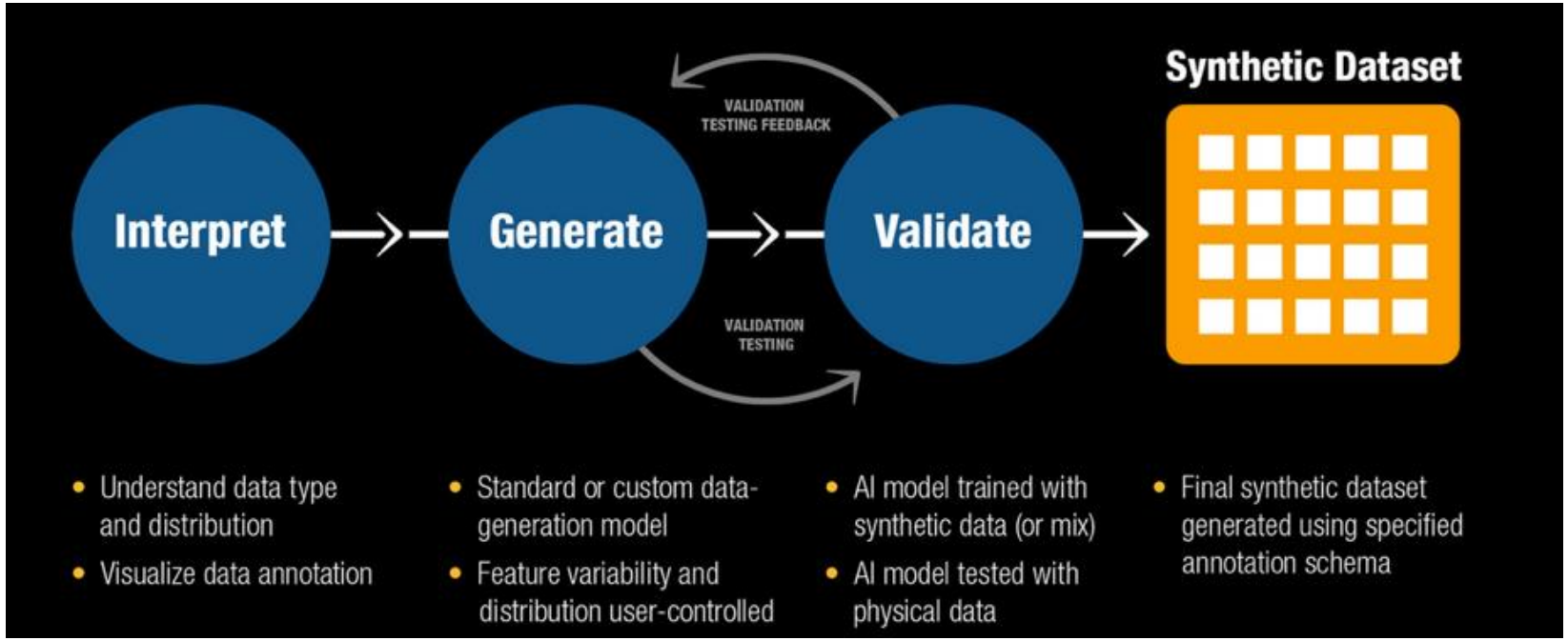
REUSE OF DATA FOR SCIENTIFIC AND MEDICAL RESEARCH: A FRAGMENTED SCENARIO

Although the choice to adopt a Regulation, in lieu of a Directive, was mainly aimed at preventing any fragmentation of the rules on the circulation and the protection of personal data within the European Union, many member States are however adopting their own laws to implement the GDPR in its entirety or, in some cases, to adapt the national frameworks to the new rules set forth in this Regulation.

The EU Commission highlighted that «*when adapting their national legislation, Member States have to take into account the fact that any national measures which would have the result of creating an obstacle to the direct applicability of the Regulation and of jeopardizing its simultaneous and uniform application in the whole of the EU are contrary to the Treaties*».

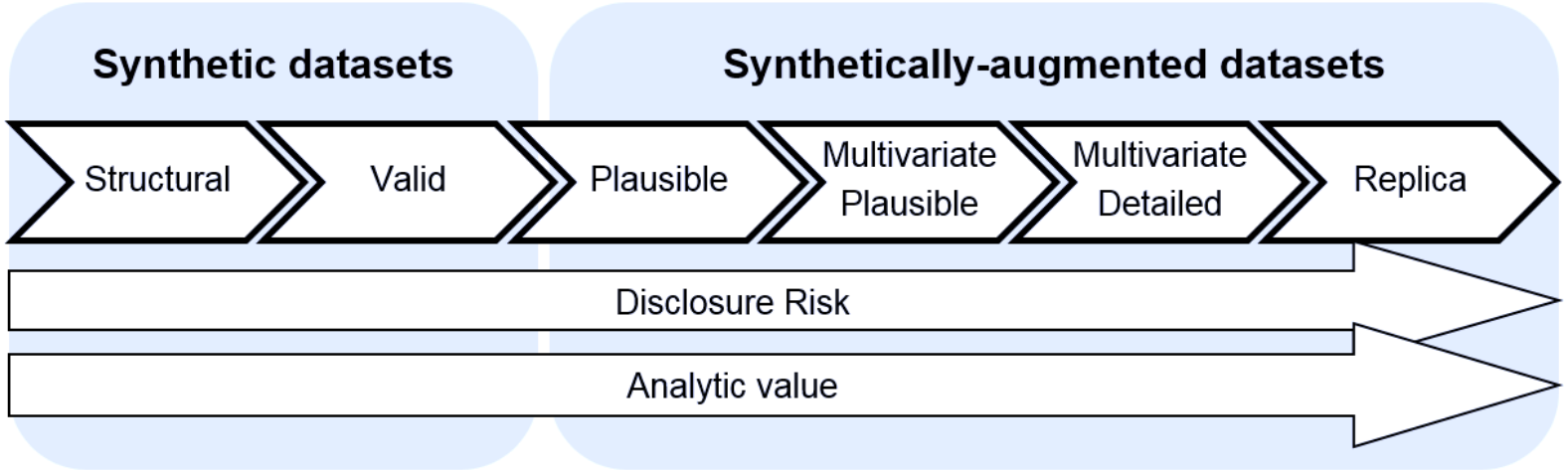
SYNTHETIC DATA

Synthetic data are generated using a combination of aggregate statistics from a known population. Using these inputs, virtual patients are created from scratch by drawing from the distributions, so that a significant amount of realistic data can be generated with an almost-zero risk of being able to identify the original data subjects.



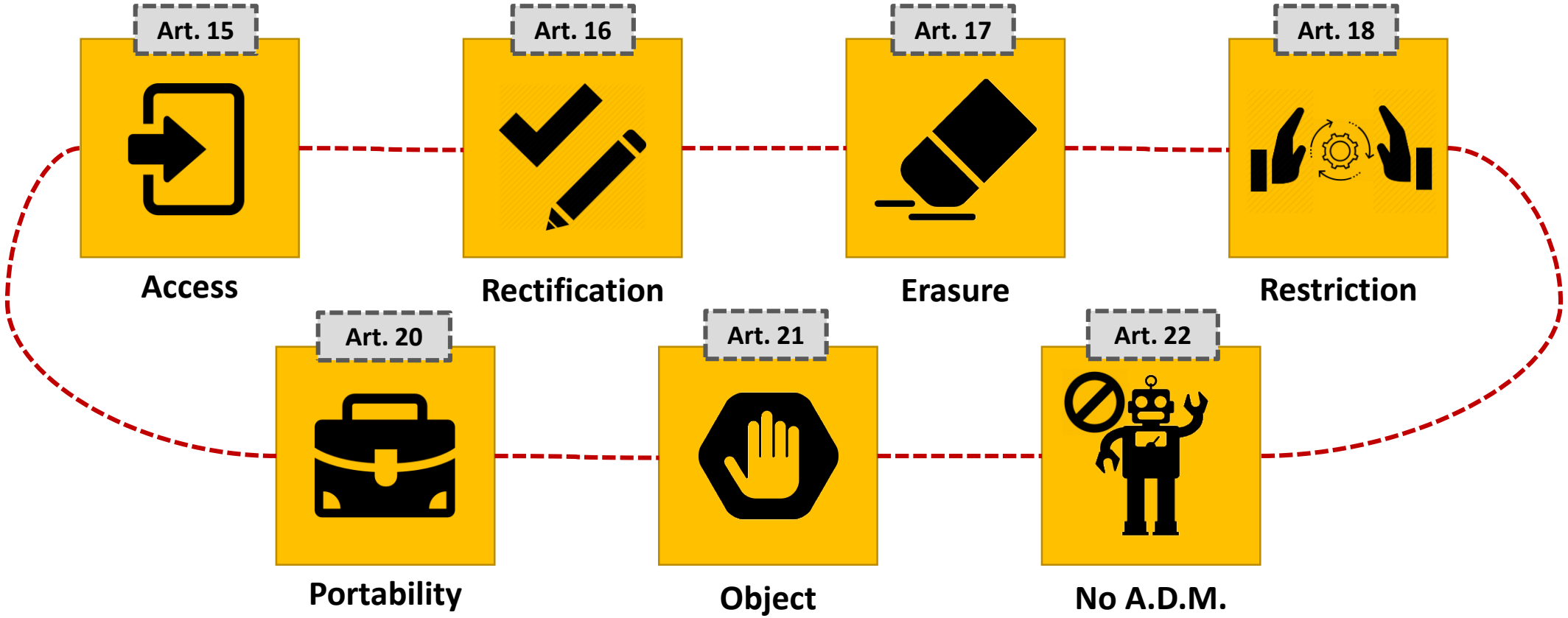
SYNTHETIC DATA

These data are indeed totally made-up and do not contain any of the original identifiable information. They are generated after the density function of the attributes in the original dataset is identified and their parameters has been estimated. Then for each attribute, privacy protected series are generated by randomly picking up the values from said estimated functions. Multiple imputation and bootstrap methods are few classical techniques used to generate fully synthetic data. These data, automatically generated by making use of machine learning algorithms, are based on recursive conditional parameter aggregation, operating within global statistical models which, by definition, do not allow any personal re-identification of original individual datasets.



This image is taken from the *ONS methodology working paper series number 16 - Synthetic data pilot*

DATA SUBJECTS' RIGHTS



Where personal data are processed for scientific research purposes, Union or Member State law may provide for additional derogations from the rights referred to above, subject to the conditions and safeguards set forth by Art. 89 of the GDPR, when such rights are likely to render impossible or seriously impair the achievement of the research and such derogations are necessary for the fulfilment of the relevant purposes

Thanks for your attention

PANETTA& ASSOCIATI

STUDIO LEGALE

Avv. Lorenzo Cristofaro

***Partner* – Panetta & Associati**

Via Arenula, 83

Roma, 00186

l.cristofaro@panetta.net

www.panetta.net